UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/724,034	11/26/2003	Markus Jakobsson	081004.179 US2	7279

7590 12/12/2007

Wilmer Cutler Pickering Hale and Dorr LLP
60 State Street
Boston, MA 02109

EXAMINER	
LEMMA, SAMSON B	
ART UNIT	PAPER NUMBER
2132	

MAIL DATE	DELIVERY MODE
12/12/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/724,034	JAKOBSSON ET AL.	
	Examiner	Art Unit	
	Samson B. Lemma	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 August 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *2-85* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *2-85* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This is in reply to amendment after a non-final office action, filed on August 24, 2007. Claim **1 is previously canceled and independent claims 2 and 73 are amended. No other claim is canceled, thus claims 2-85** are pending/ examined.

Priority

2. This application claims priority of a provisional application, application No. 60/429754 filed on **November 27, 2002**. Therefore, the effective filling data for the subject matter defined in the pending claims of this application is **11/27/2002.**

Response to Arguments

3. Applicant's argument filed on August 24, 2007 have been fully considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. **Claims 2 and 73** are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claims 1 and 73 are indefinite because each claims recites the following broad limitation "...**event state data representing an**

occurrence of reportable event concerning a condition of authentication device" which does not contain a specific/well defined meaning, because in view of the applicant's specification as it is disclosed on the applicant's publication paragraph 0011, such limitation could be interpreted in a variety ways with out a specific and well defined meaning.

For instance, Applicant's specification on paragraph 0011, recites the following,

"A reportable event is an event other than events associated with the normal operation of an authentication method (and that can be reported to the verifier). Thus, for example, a reportable event would not include an event reporting a request for an authentication code. A reportable event ***could be, on the other hand, an event that is at least one of an anomalous, extraordinary, remarkable, unusual, and the like.*** *A reportable event also could be any sort of event that can be detected and/or communicated by or to the device.* ***Example reportable events include: device tampering; an event external to the device detected by the device; an environmental event, such as temperature exceeding or falling below a threshold; static discharge; high or low battery power; geographic presence at a particular location; confidence level in a biometric reading; and so on.*** *A reportable event may also* ***provide an indication of the likelihood that the security of the authentication system has been compromised or the likelihood that the authentication device has or will develop an operational problem (e.g., the condition of the authentication device). A reportable event can be the cumulative effect of multiple past events. A reportable event also can be the device operational status."***

In view of the above specification, it is undoubtedly clear that such limitation is so broad and could be any one of the above examples, provided by the applicant's. For this reason/s, the above claims requires a proper amendment so that the claim limitation/s become specific and has a well-defined meaning.

For the sake of examination, the office interprets the limitation in any one of the above example/s provided by the applicant's specifications.

6. **Claims 3-25 and 74-82** depend from the rejected claims 1 and 73 and include all the limitations of the respective claims, thereby rendering those dependent claims indefinite.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. **Claims 2-72** are rejected are rejected under 35 U.S.C. 103(a) as being unpatentable over **Secure computing corporation: "Authentication Reference Guide"** (Hereinafter referred as **Secure Computing)** (Publication date: April 9, 2002) (Pages 1-18, XP002283680, Submitted with the IDS) in view of Tanaka et al (Hereinafter referred as **Tanaka)** (U.S. Patent No. 7,024,698 B2, filed on April 27, 2001)

> Examiner has pointed out particular references contained in the prior arts of record in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. Applicant should consider the entire prior art as applicable as to the limitations of the claims. It is respectfully requested from the applicant, in preparing the response, to consider fully the entire references as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the examiner.

9. **As per independent claims 2, 26, 43 and 57 Secure Computing discloses a method for generating an identity authentication code** *[See pages 11-12 and 14-16, "dynamic password"]* **associated with an authentication device,** *[See pages 11-12 and 14-16, "Authenticator/token"]* **comprising the steps of:**

- **Providing event state data that specifies a condition of the authentication device;** *[See pages 11-12 and 14-16, "challenge/response"]* ; **and**
- **Generating an identity authentication code** *[See pages 11-12 and 14-16, "dynamic password"]* **that depends at least in part on (ii) the event state data,** *[See pages 11-12 and 14-16, "response"]* **and (ii) a secret associated with the device. [***See pages 11-12 and 14-16, "pin"].*

Furthermore on dependent claim 3, and on the abstract of the "applicant's submitted specification", it has been recited that the identity authentication code further depends **on dynamic values** and on dependent claim 4, it has been further recited that such dynamic value includes **a challenge.**

Secure Computing, discloses such limitation/s "dynamic value", *[See pages 11-12 and 14-16, "challenge"]*

Furthermore, **Secure computing on Page 15** discloses the following "If the token is stolen, the thief cannot retrieve valid passwords from the token without the PIN; what's more, as soon as the token is reported stolen, the administrator can immediately disable it. This type of token can be configured for synchronous or asynchronous authentication."

Secure Computing does not explicitly disclose,

providing event state data representing an occurrence of a reportable event concerning a condition of the authentication device; and/or providing event state

data that is a security indicator for an authentication system of which the authentication device is a component or providing event state data that specifies information about the user of the authentication device or information about environmental condition associated with the authentication device.

However, in the field of endeavor **Tanaka et al discloses,** *providing event state data representing an occurrence of a reportable event concerning a condition of the authentication device; and/or providing event state data that is a security indicator[See, the sensor on figure 7, ref. Num "708" and "warning", column 7, lines 5-10] for an authentication system [See figure 7, ref. Num "702"] of which the authentication device is a component.; [See column 3,lines 39-50 and column 4, lines 5-8 and figure 3, ref. Num "302-308"] (On column 3, lines 39-50, the following has been discloses. "Step 308: Judgement is made for the situating condition of* ***the portable information-processing device/authentication device*** *as to whether it is currently normal or abnormal based on a check result of the outputs of the sensor 205 and the check result of the locational information output by the GPS module 206/environmental condition associated with the device. In checking the acceleration, vibration, and change in inclination, judgments are made as to whether or not they exceed presumed ranges. In checking the locational information, judgement is made as to whether the information-processing device has been moved beyond a presumed area. Determination as to whether the situating condition of the portable information-processing device is normal or abnormal is made accordingly based upon results of these judgements." Furthermore on Column 4, lines 5-8, the following has also been disclosed, "In one instance,* ***a condition of the radio communication is checked,*** *and it proceeds to the step 312 if the destination device is found located outside of the communication range." Such communication signals used for making the judgements meets the limitation recited as "representing an occurrence*

of a reportable event concerning ***a condition of authentication device****". Furthermore if the authentication device is abnormal then it may be the case that it is stolen by illegitimate user/s meets the limitation recited as "specifying information about the user of the authentication device")*

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the features such as *"providing event state data representing an occurrence of a reportable event concerning a condition of the authentication device"* as per teachings Tanaka in to the method of as taught by **Secure Computing** for providing protection of data in the authentication device and achieving confidentiality when the authentication device is tampered or stolen. [See Tanaka, abstract]

10. **As per dependent claims 3, 27, 44 and 58 the combination of Secure computing and Tanaka discloses a method as applied to claims above. Furthermore secure computing discloses the method wherein, the identity authentication code further depends on a dynamic value.** *[See pages 11-12 and 14-16, "challenge"]*

11. **As per dependent claims 4, 28, 45 and 59 the combination of Secure computing and Tanaka discloses a method as applied to claims above. Furthermore Secure computing discloses the method, wherein the dynamic value includes one or more of a time value, a challenge, and a counter.** *[See pages 11-12 and 14-16, "challenge" and see on page 12,* ***"time-synchronous authentication*** *and on page 11, see "The crypto-algorithm incorporated in the token uses a* ***counter that*** *stays "in sync" with the server based on the number of passwords generated]*

12. **As per dependent claims 5 the combination of Secure computing and Tanaka discloses a method as applied to claims above. Furthermore Tanaka discloses the method, wherein the condition of the authentication device includes information about whether the device has been subjected to tampering. [See abstact, "stolen"]**

13. **As per dependent claim 6, the combination of Secure computing and Tanaka discloses a method as applied to claims above. Furthermore secure computing discloses the method, further including changing the event state data when the condition of the authentication device changes** *[See pages 11-12 and 14-16, "response/challenge"]*

14. **As per dependent claim 7 the combination of Secure computing and Tanaka discloses a method as applied to claims above. Furthermore Secure computing discloses the method, wherein the condition of the device is covertly encoded in the identity authentication code.** *[See pages 11-12 and 14-16],* (Generating an identity authentication code *or "dynamic password"* that depends at least in part on (i) a dynamic value/condition of the device or *"challenge"* (ii) the event state or, *"response"* and (iii) a secret associated with the device or *"pin" meets the recitation of the limitation)*

15. **As per dependent claim 8 the combination of Secure computing and Tanaka discloses a method as applied to claims above. Furthermore Secure computing discloses the method, wherein the event state data***[See pages 11-12 and 14-16, "challenge"]* **is derived from an associated event secret. [***See pages 11-12 and 14-16, "pin"] (the challenge is prompted to the user after the pin is entered by the user meets the limitation of the challenge is derived from the an associated pin/event secret)*

16. **As per dependent claims 9-10 and 30-34 the combination of Secure computing and Tanaka discloses a method as applied to claims above. Furthermore Secure computing discloses the method, further including periodically changing the event secret. [***See pages 11-12 and 14-16, "pin"] ("this is an inherent features of authentication device which uses a pin", in any authentication system pins are periodically changing for security purposes)*

17. **As per dependent claim 11 the combination of Secure computing and Tanaka discloses a method as applied to claim above. Furthermore, Secure computing discloses the method further including changing the event secret when the condition of the authentication device changes. [***See pages 11-12 and 14-16, "pin"] ("this is an inherent features of authentication device which uses a pin", in any authentication system pins are periodically changing for security purposes)*

18. **As per dependent claims 12-13 the combination of Secure computing and Tanaka discloses a method as applied to claims above. Furthermore Secure computing discloses the method, wherein the event state data includes one or more event state bits, a subset of bits** *[See pages 11-12 and 14-16, "challenge"]* **being employed in generating identity authentication codes** *[See pages 11-12 and 14-16, "dynamic password"]* **for different time intervals [Pages 12-13]** *(Time-synchronous authenticators also generate unique, dynamic passwords at fixed intervals, usually one per minute.)*

19. **As per dependent claims 14-16 the combination of Secure computing and Tanaka discloses a method as applied to claims above. Furthermore secure computing discloses the method, wherein the condition of the authentication device includes information about whether a battery supplying power to the authentication device has fallen below an expected power level.** *[See page 15] (See*

for instance just one type of authentication device driven by a batter on page 15, and an indication that battery of these devices are fallen below an expected power level is an inherent feature in any small handheld battery driven devices.)

20. **As per dependent claims 17, 35-37, 49 and 65, the combination of Secure computing and Tanaka discloses a method as applied to claims above. Furthermore Secure computing discloses the method, wherein the identity authentication code** *[See pages 11-12 and 14-16, "dynamic password"]* ***further depends on one or more of a PIN, a password,*** **[***See pages 11-12 and 14-16, "pin"]* ***data derived from a biometric observation,****[See page 17]* ***user data, verifier data and a generation value*** *[See pages 11-12 and 14-16, "challenge/response"]*

21. **As per dependent claims 18-19 and 29, 42, 50, 56, 66 and 72 the combination of Secure computing and Tanaka discloses a method as applied to claims above. Furthermore Secure computing discloses the method, further including, before generating the authentication code** *[See pages 11-12 and 14-16, "dynamic password"]* ***receiving user input data*** *[See pages 11-12 and 14-16, response or pin"],* ***wherein the user input data is at least one of a PIN, a password,*** *[See pages 11-12 and 14-16, "pin"]* **and biometric data** *[See page 17]*

22. **As per dependent claims 20-24, 38-41,51-55, 67-71 the combination of Secure computing and Tanaka discloses a method as applied to claims above. Furthermore Secure computing discloses the method, further including, transmitting the identity authentication code to verifier.***["See pages 14-17, "authentication"]*

23. **As per dependent claim 25 the combination of Secure computing and Tanaka discloses a method as applied to claims above. Furthermore Secure**

computing discloses the method, further including the step of displaying the identify authentication code on the device. *[See page 15]*

24. **As per dependent claims 46-48 and 60-64 the combination of Secure computing and Tanaka discloses a method as applied to claims above. Furthermore Secure computing discloses the method, wherein the information about the user includes where the user is located. [See page 1,** *"behavioral measurement of the user, or determine that the user is located at a place..")*

25. **Claims 73-85** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Smithies et al** (Hereinafter referred as **Smithies)** (U.S. Patent No. 6,091,835), Patent Date: 07/18/2000) **in view of Tanaka et al** (Hereinafter referred as **Tanaka)** (U.S. Patent No. 7,024,698 B2, filed on April 27, 2001)

26. **As per independent claims 73, 83-85 and dependent claims 74-77 and 80-82 Smithies discloses a method for verifying the correctness of an identity authentication code,**

comprising:

- **Receiving authentication information including the identity authentication code generated by an authentication device that depends on (i) a secret associated with the device, and (ii) event state data that specifies a condition of the authentication device;**[See claims 1 and 58] *(Claim 1 recites the following which meets the limitation of the above recitation, "a computer system for creating a secure, tamper-resistant electronic transcript which memorializes the events of a user's affirmation, through the entry of a signature token, of an electronic transaction having terms, the system comprising: a. a transaction application module enabling an affirming party to create an electronic transaction; b. a transcript generator module; and c.*

a signature token verification module accepting the signature token from the affirming party." Furthermore claim 58 discloses the following which also meets the above recitation, "a computer based system for recording a series of acts constituting the signing of an electronic document and assuring an affirming party's intent, comprising: presentation means presenting an electronic document to be signed to the affirming party, the presentation means allowing the affirming party to electronically examine the document by accepting an at least one document review affirming party input command and displaying an at least one portion of the document in accordance with the at least one document review affirming party input command, the presentation means displaying a declaration of intention indicating the intention of the affirming party towards the document; verification means verifying the identity of the affirming party by requesting identity information from the affirming party and accepting identity information from the affirming party; checksumming means creating a document checksum of the document;ceremony generating means generating ceremony information from: the presentation of the document to the affirming party; the at least one document review affirming party input command and the at least one portion of the document displayed)

- **Verifying the correctness of the identity authentication code, and determining the condition of the authentication device in response to the received identity authentication code.** [See claims 1 and 58] *(Claim 1 recites the following which meets the limitation of the above recitation, "a signature token verification module accepting the signature token from the affirming party, verifying the signature token and transmitting a verification signal to the transcript generator module; wherein the transcript generator module accepts the terms, confirms the acceptance of the terms by presenting prompts, allows the affirming party to affirm the terms, gathers forensic data surrounding the affirming party's affirmation and stores information related to the prompts, the forensic data and the verified token as separate data entities in a tamper-*

resistant transcript object." Furthermore, claim 58 discloses the following which also meets the above recitation, "verification means verifying the identity of the affirming party by requesting identity information from the affirming party and accepting identity information from the affirming party; checksumming means creating a document checksum of the document; ceremony generating means generating ceremony information from: the presentation of the document to the affirming party; the at least one document review affirming party input command and the at least one portion of the document displayed; and the at least one identity input event relating to the identity information; and storing the identity information, document checksum and ceremony information in a transcript object.")

Smithies does not explicitly discloses

event state data representing an occurrence of a reportable event concerning a condition of the authentication device; and/or providing event state data that is a security indicator for an authentication system of which the authentication device is a component or providing event state data that specifies information about the user of the authentication device or information about environmental condition associated with the authentication device.

However, in the field of endeavor **Tanaka discloses,** *providing event state data representing an occurrence of a reportable event concerning a condition of the authentication device; and/or providing event state data that is a security indicator[See, the sensor on figure 7, ref. Num "708" and "warning", column 7, lines 5-10] for an authentication system [See figure 7, ref. Num "702"] of which the authentication device is a component.; [See column 3,lines 39-50 and column 4, lines 5-8 and figure 3, ref. Num "302-308" and column 7, lines 5-10] (On column 3, lines 39-50, the following has been discloses. "Step 308: Judgement is made for the situating condition of* ***the portable information-processing***

device/authentication device *as to whether it is currently normal or abnormal based on a check result of the outputs of the sensor 205 and the check result of the locational information output by the GPS module 206/environmental condition associated with the device. In checking the acceleration, vibration, and change in inclination, judgments are made as to whether or not they exceed presumed ranges. In checking the locational information, judgement is made as to whether the information-processing device has been moved beyond a presumed area. Determination as to whether the situating condition of the portable information-processing device is normal or abnormal is made accordingly based upon results of these judgements." Furthermore on Column 4, lines 5-8, the following has also been disclosed, "In one instance,* ***a condition of the radio communication is checked,*** *and it proceeds to the step 312 if the destination device is found located outside of the communication range." Such communication signals used for making the judgements meets the limitation recited as "representing an occurrence of a reportable event concerning* ***a condition of authentication device****". Furthermore if the authentication device is abnormal then it may be the case that it is stolen by illegitimate user/s meets the limitation recited as "specifying information about the user of the authentication device")*

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the features such as "*providing event state data representing an occurrence of a reportable event concerning a condition of the authentication device*" as per teachings Tanaka in to the method of as taught by **Smithies** for providing protection of data in the authentication device and achieving confidentiality when the authentication device is tampered or stolen. [See Tanaka, abstract]

27. **As per dependent claim 78 the combination of Smithies and Tanaka discloses a method as applied to claims above. Furthermore Smithies discloses the method wherein the authentication information further includes user identifier.** *[See column 43 and claim 43]*

28. **As per dependent claim 79 combination of Smithies and Tanaka discloses a method as applied to claims above. Furthermore Smithies discloses the method wherein the authentication information further includes at least one of a PIN, a password, and biometric data.** *[See column 43 and claim 43]*

Conclusion

29. The previous prior art made of record and not relied upon is considered pertinent to applicant's disclosure.(See PTO-Form 892).

a. **U.S. Patent No. 5, 251,259** discloses a method for generating an identify authentication code using different event state features as it is described on figure 3 and claim 1) comprising the steps of:

- storing events in an authentication device (See for instance "frequency of use")
- modifying the event state in response to an event ("See for instance "respone") and
- generating an identify authentication code that depends on at least in part on a dynamic value (day), the event state (number of usage) and a secret (Pin) associated with authentication device. Furthermore, the method discloses dynamic value associated with a time period or interval (See for instance, column 2)

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-873-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SAMSON LEMMA
S.L.
12/01/2007

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100